Time Management Technical Exchange

Jan Filsinger

Trusted Information Systems, Inc.

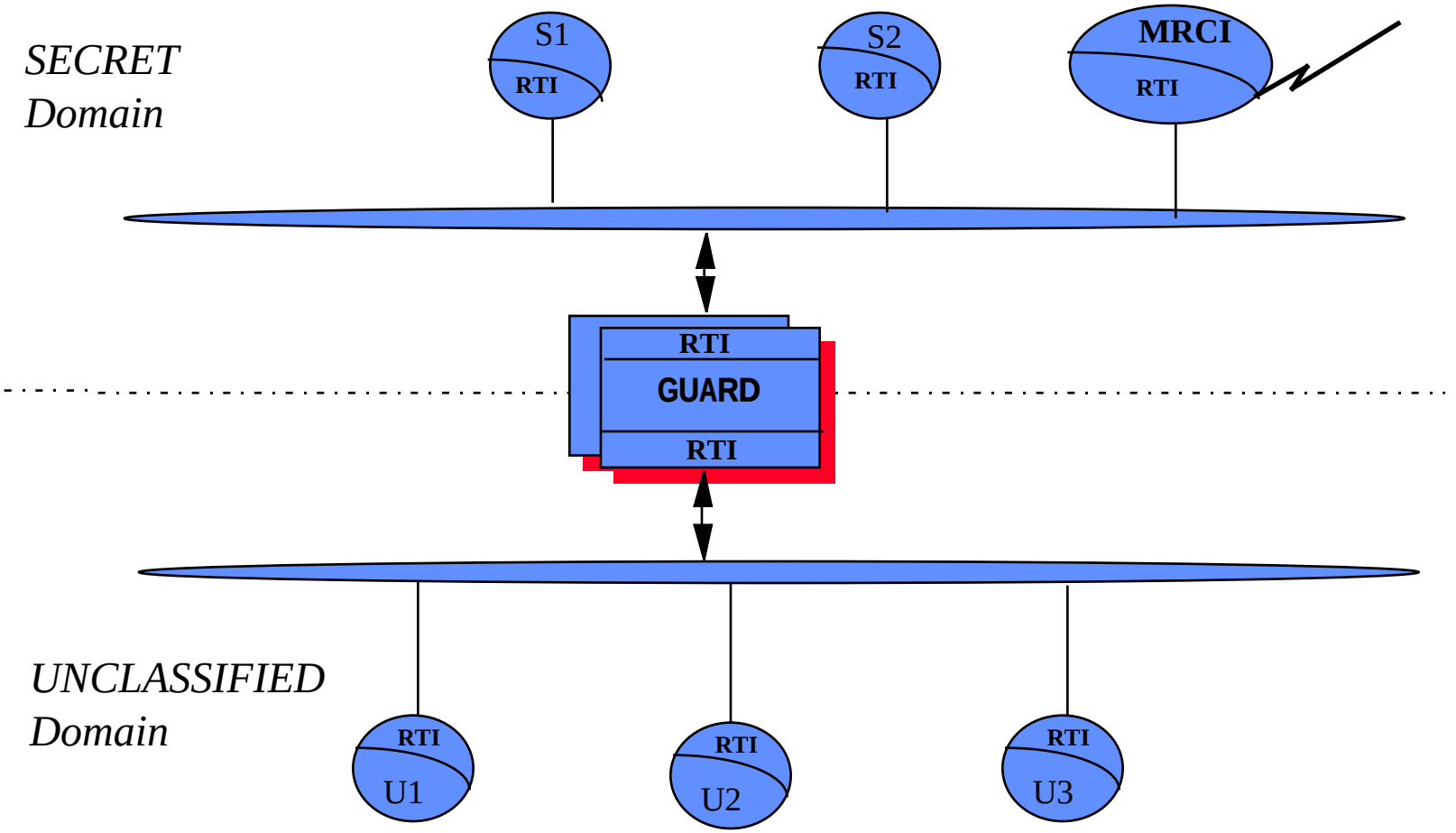
janf@tis.com

16 December 1996

Overview

- **HLA Secure Combined Federation Architecure**
- **RTI-Guard Interface Analysis**
  - **Federation Management**
  - **Declaration Management**
  - **Object Mangement**
  - **Ownership Management**
  - **Time Management**
  - **Data Distribution Management**
- **Summary**

HLA Secure Combined Federation



HLA Secure Combined Federation

- **Combined Federation**
  - **Two or more**
    - **security domains**
    - **SOMs**
    - **FOMs**
    - **Federation executions**
    - **RTIs**
  - **One Combined FOM**
    - **Data that is shared among the federations**

HLA Security Guard

- **HLA Security Guard Gateway Functions**
  - **Multiple federation executions**
  - **RTI service interpretation/API**
  - **Implementation**
    - **Not trusted**
    - **Reuse of ‘middle ware’**
- **HLA Guard Security Functions**
  - **Object Id mapping**
  - **Data mapping**
  - **Data sanitization**
  - **Implementation**
    - **Trusted**
    - **Possible reuse of existing guard technology**

- Secure logon + audit capability

- Rule Creation/modification

HLA Security Guard

- **HLA Guard System Functions**
  - **Review erred data**
  - **Error Processing**
    - **Detect and reject faulty data and RTI services**
    - **Detect security anomalies**
  - **Input federation and security configuration data**
  - **Automatic shutdown on critical security conditions**

RTI-Guard Interface Analysis

- **Objectives**
  - **Identify Guard-RTI gateway operations**
  - **Identify critical security operations**
  - **Identify problem areas**

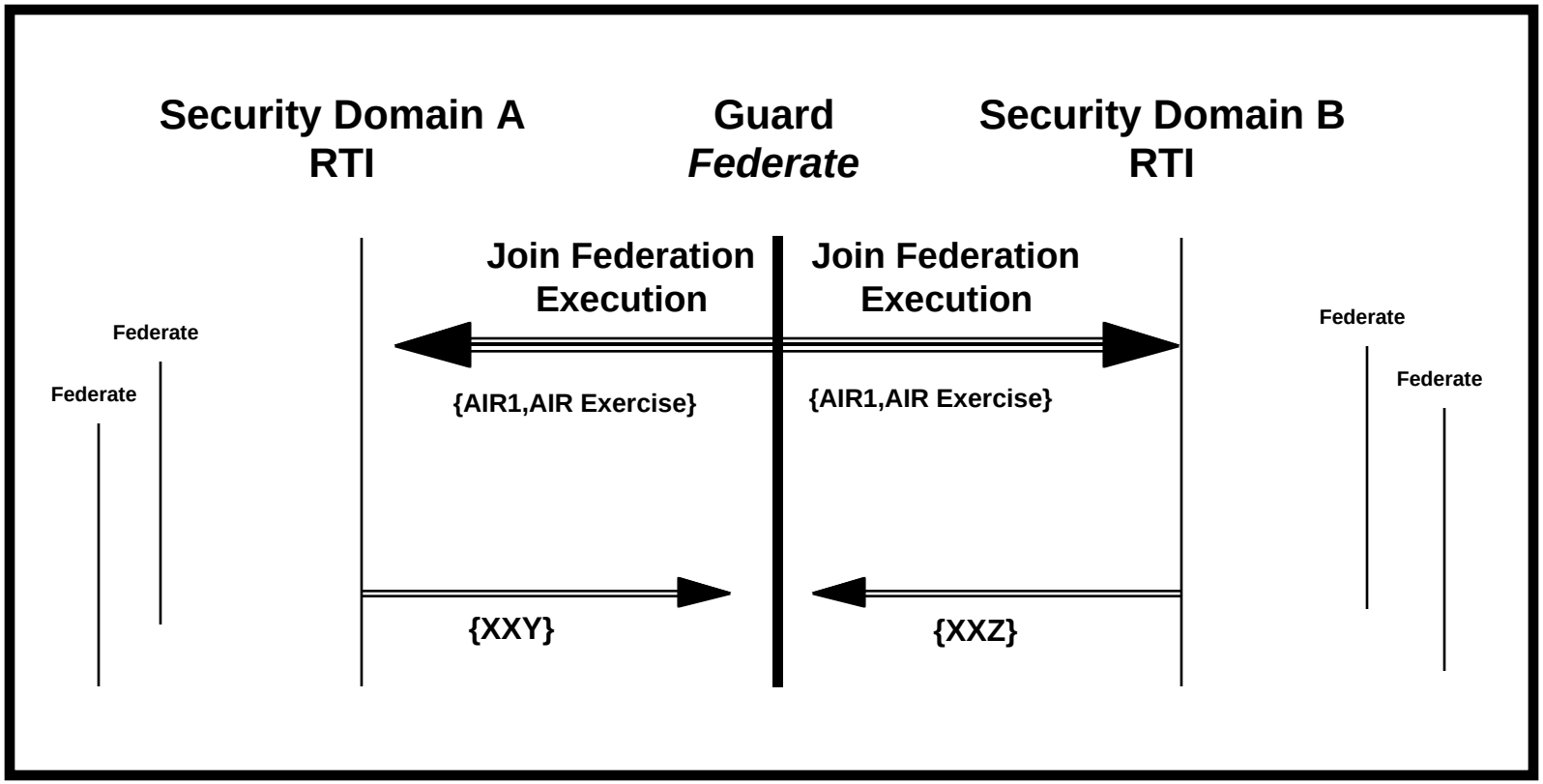
RTI-Guard Interface Analysis

- **Federation Management**
  - **Provides control over the federation execution**
  - **Classified data is not transferred using these services**
  - **Security concerns**
    - **Signaling channels could be exploited during pause/ resume commands -- this risk can be mitigated through audit**
    - **Federate identification is performed by the RTI, not authentication**
  - **Resign Federation**
    - **Guard needs to know who is still part of the federation execution**

tis

RTI-Guard Interface Analysis

Security Guard as an Federate



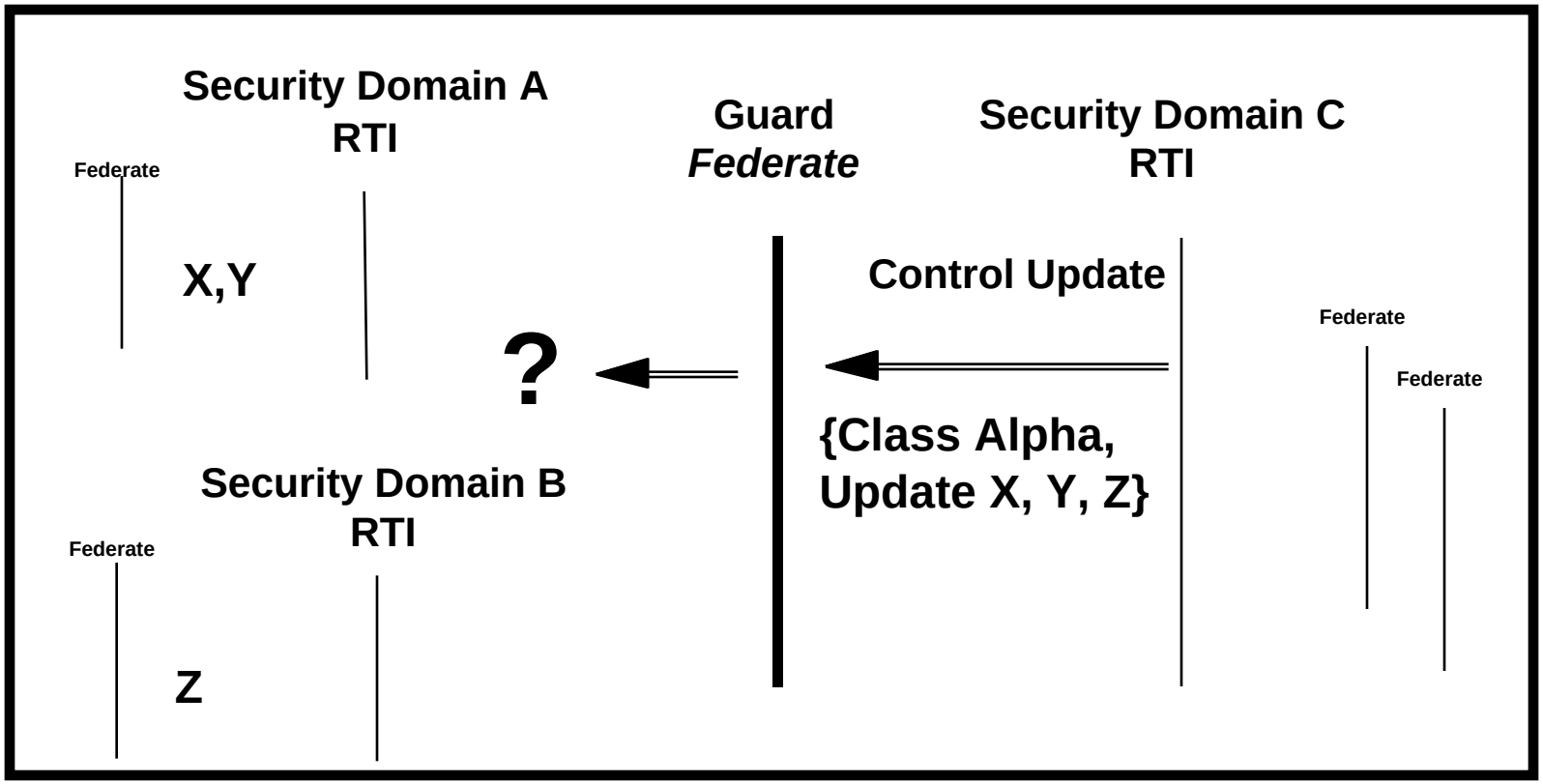
RTI-Guard Interface Analysis

- **Declaration Management**
  - **Federate declaration to the RTI the capability to generate & receive objects**
  - **Guard required to sanitize data for these services**
  - **Security concerns**
    - **unexpected or incorrectly formatted data will be rejected**
    - **Error handling causing signaling channels**
    - **Complexity of rule set**
    - **Correctness of rule set**
    - **Polyinstantiated object attributes**
  - **Control Updates**
    - **Guard does not have a method to find attribute owner**

tis

RTI-Guard Interface Analysis

Control Update



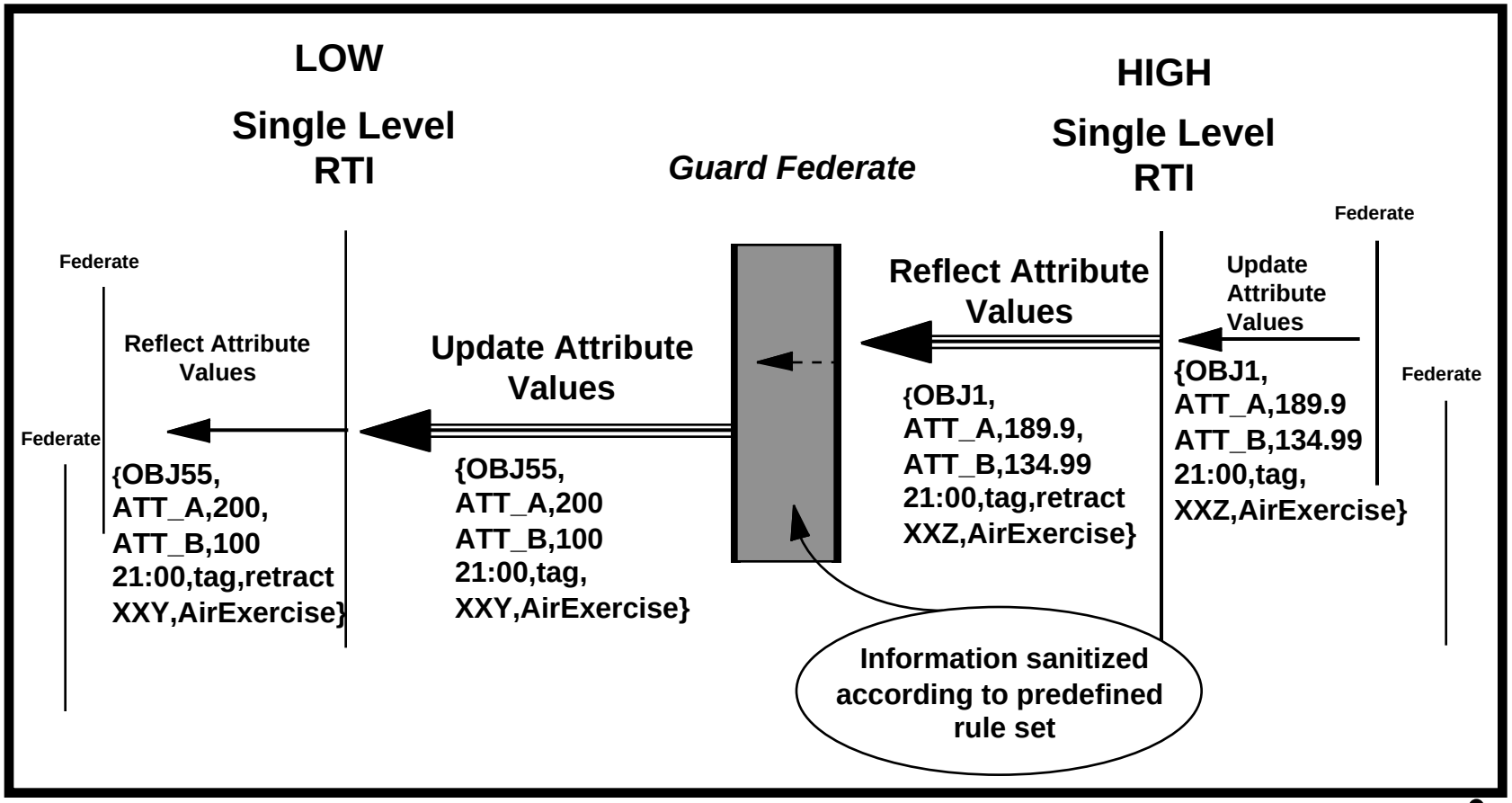
RTI-Guard Interface Analysis

- **Object Management**
  - **Support creation, modification and deletion of objects and interactions**
  - **Guard will have to sanitize data to support these services**
  - **Guard will 'appear' to own all objects required in other security domains**
  - **Security concerns**
    - **Control and distribution of object IDs**
    - **Guard apparent ownership of data**
  - **Provide Attribute Value Update**
    - **Similar conditions as Control Updates (RTI Initiated)**
  - **Delete Object**
    - **Must have the PrivToDelete for all objects crossing security domains**

tis

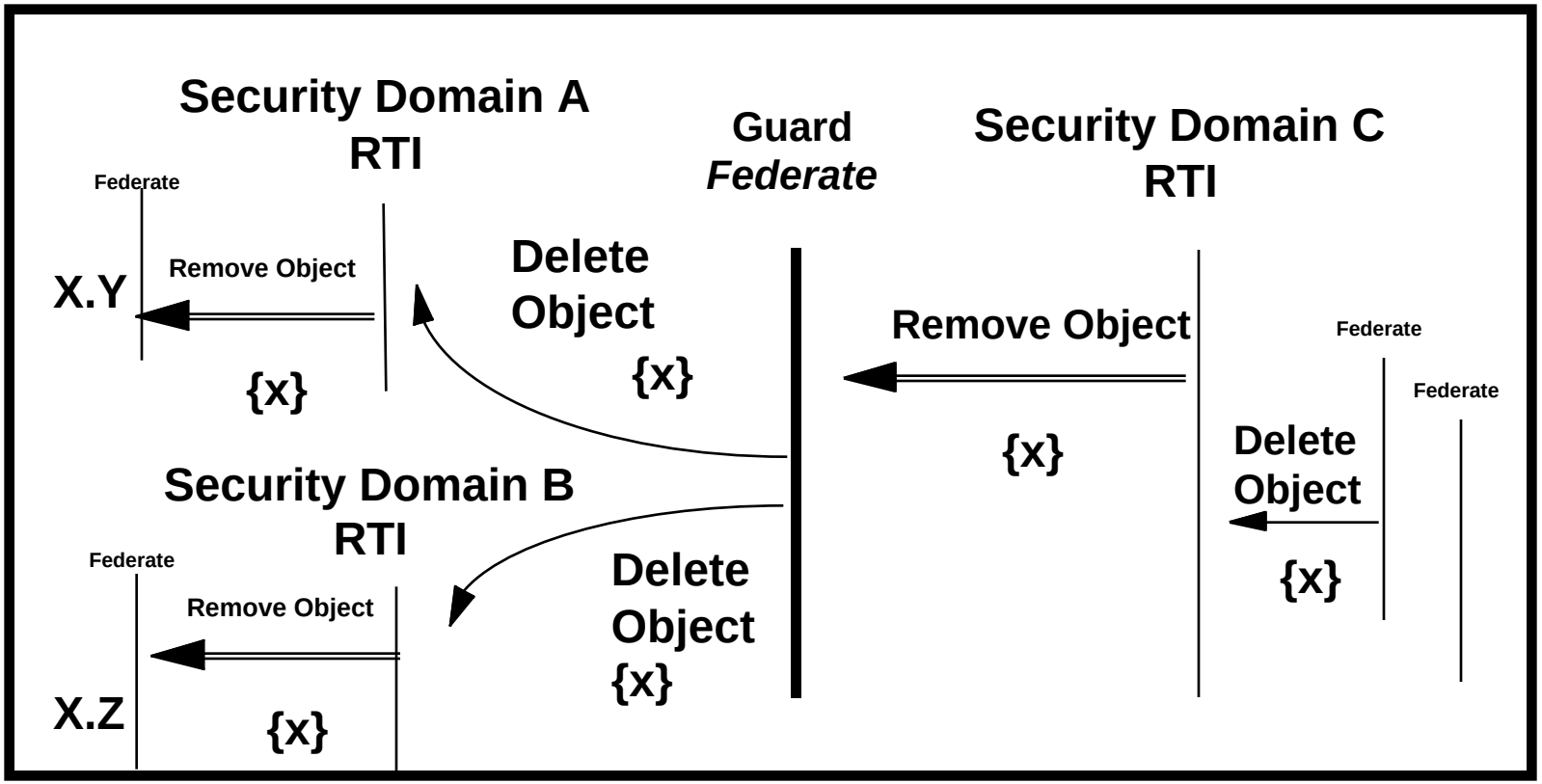
RTI-Guard Interface Analysis

Object Transfer



RTI-Guard Interface Analysis

Delete Object



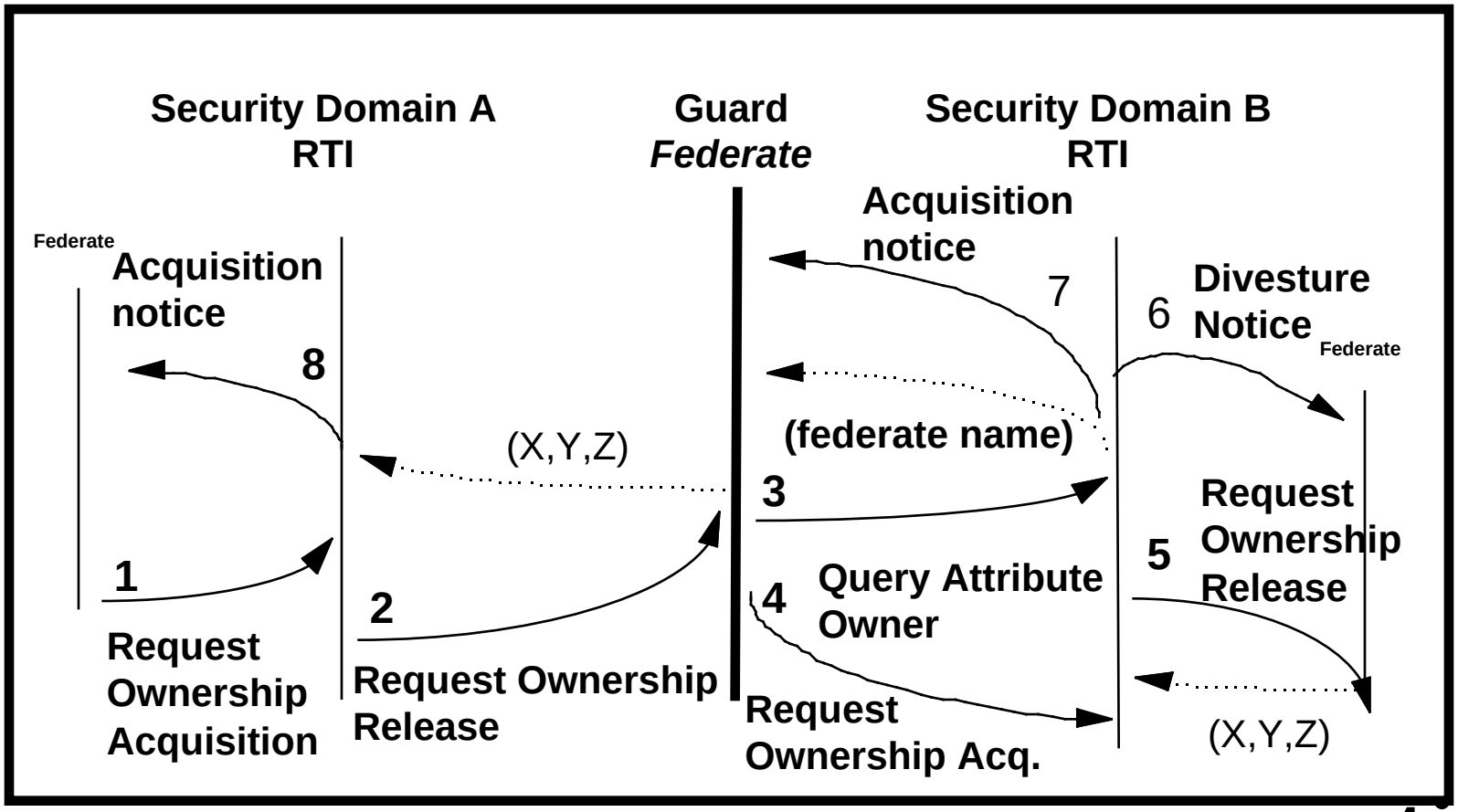
RTI-Guard Interface Analysis

- **Ownership Management**
  - **Provide the ability for a federate to transfer ownership of object attributes**
  - **No data sanitization is required to support these services**
  - **Security Concerns**
    - **Guard needs to know who really owns the object (RTI has this knowledge)**
    - **Specific object ownership transfers must be specified in the FOM -- will not be dynamic**
  - **Ownership transfer is complex**

tis

RTI-Guard Interface Analysis

Ownership Transfer



RTI-Guard Interface Analysis

- **Time Management**
  - **Controls the advancement of time in a federation**
    - **Best Effort**
    - **Timestamp**
  - **Guard implementation of time management services require a modification to the current Interface Spec**
  - **Security Concerns**
    - **Synchronization between RTIs**
    - **Guard retaining state information**
  - **Example Commands**
    - **Request Federate Time, Request LBTS, Set Lookahead, Time Advance Request, Request Lookahead**

tis

RTI-Guard Interface Analysis

- **Time Management Issues**
  - **Security**
    - **Time management services do not require the guard federate to perform data sanitization**
    - **Manipulation of the time services can create covert channels.**
  - **Time synchronization between information domains or RTIs is required.**
  - **Current RTI Interface Spec does not support Combined Federations.**

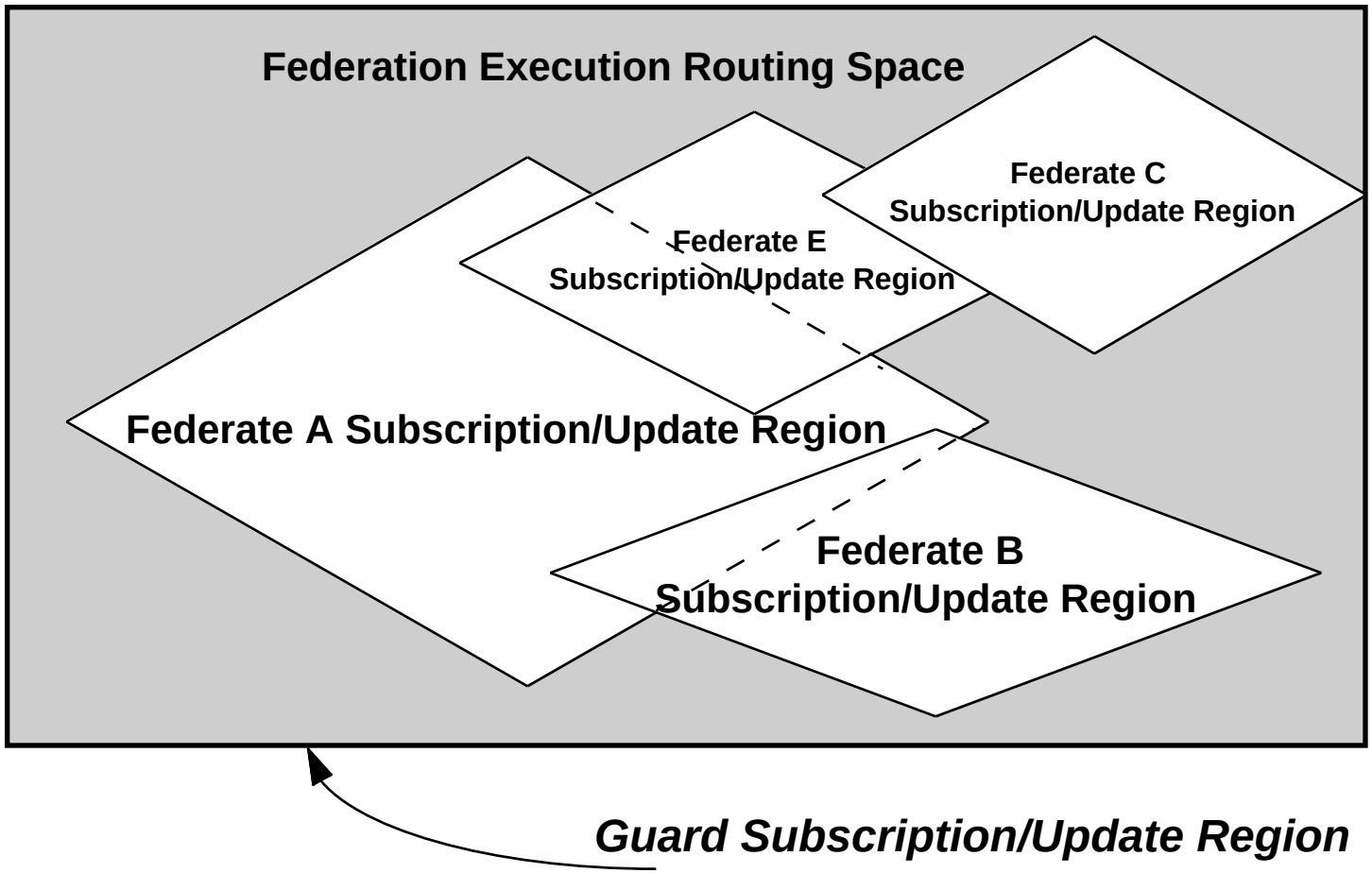
tis

RTI-Guard Interface Analysis

- **Data Distribution**
  - **Provides the means for the RTI to distribute data efficiently**
  - **Guard interplay with these services are TBD**
  - **Example Commands**
    - **Create Update Region, Create Subscription Region,**
    - **Associate Update Region, Change Thresholds, Modify Region**
    - **Delete Region**

tis

Data Distribution



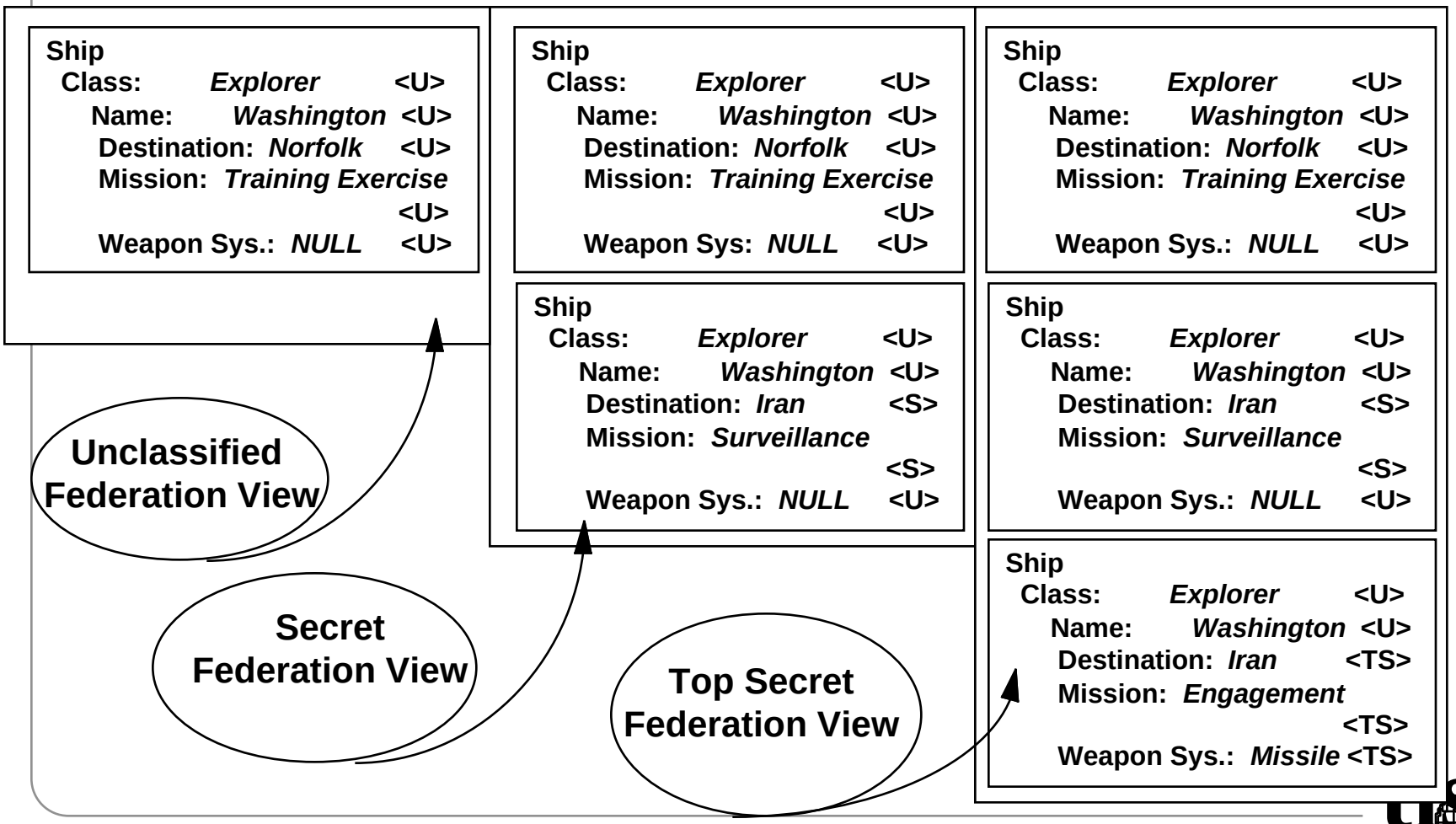
Summary

- **Data Issues**
  - **Sanitization Rules -- Developed in the Combined Federation process**
  - **Data aggregation -- Addressed in Combined Federation process**
  - **Multilevel objects (Polyinstantiation)**
    - **Higher federates will receive object attributes that will have multiple values distinguished only by classification level**
      - **Example: Multiple versions of ground truth, multiple versions of perceived truth**

tis

Polyinstantiated Data

Security Guard View of Combined Federation Data



Summary

- **Architecture Issues**
  - **Signaling channels from high domain to lower domains**
  - **Synchronization of domains**
  - **Number of guards**
  - **RTI**
    - **Guard is event driven**
      - **Some RTI services do not have an initiating event**
    - **Guard needs to know which security domain (or all) receives a event**
  - **Real time performance**

tis

RTI-Guard Interface Analysis